



Avaya Solution Interoperability Lab

Configuring 9600-Series SIP Phones with Avaya Aura™ Session Manager Release 5.2 – Issue 1.0

Abstract

These Application Notes describe the configuration of 9600-Series SIP Phones with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager as a Feature Server.

- Avaya Aura™ Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura™ Communication Manager operates as a Feature Server for the SIP endpoints which communicate with Avaya Aura™ Session Manager over SIP trunks.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested on this solution.

Table of Contents:

1.	Introduction.....	4
1.1.	Equipment and Software Validated.....	5
2.	Configuring Avaya Aura™ Communication Manager Feature Server.....	6
2.1.	Verify System Capabilities and Licensing.....	6
2.1.1.	SIP Trunk Capacity Check	6
2.1.2.	AAR/ARS Routing Check.....	6
2.1.3.	Configure Trunk-to-Trunk Transfers	7
2.1.4.	Enable Private Numbering.....	7
2.2.	Add Node Name of Avaya Aura™ Session Manager	8
2.3.	Configure IP Network Region	8
2.4.	Add SIP Signaling Group.....	8
2.5.	Add SIP Trunk Group	9
2.6.	Administering Numbering Plan	11
2.7.	Configure Stations	12
2.8.	Configure Off-PBX-Telephone Station-Mapping.....	13
2.9.	Save Translations.....	13
3.	Configure Avaya Aura™ Session Manager	13
3.1.	Administer SIP Domains.....	15
3.2.	Define Locations.....	15
3.3.	Add Avaya Aura™ Communication Manager Access Element.....	16
3.3.1.	Define SIP Entity for the Avaya Aura™ Communication Manager Access Element	16
3.3.2.	Define an Entity Link for Avaya Aura™ Communication Manager Access Element	17
3.3.3.	Define Routing Policy for Avaya Aura™ Communication Manager Access Element	18
3.3.4.	Define Dial Plan for calls to Avaya Aura™ Communication Manager Access Element	19
3.4.	Add Avaya Aura™ Communication Manager Feature Server.....	20
3.4.1.	Define a SIP Entity for Avaya Aura™ Communication Manager Feature Server	21
3.4.2.	Define Entity Link for Avaya Aura™ Communication Manager Feature Server	22
3.4.3.	Define Routing Policy for Avaya Aura™ Communication Manager Feature Server.....	23

3.4.4.	Define Application Sequence for Avaya Aura™ Communication Manager Feature Server	23
3.4.5.	Define Avaya Aura™ Communication Manager Feature as an Administrable Entity	24
3.4.6.	Add SIP Users.....	26
4.	Configuring Avaya Aura™ Communication Manager Access Element.....	30
4.1.	Verify System Capabilities and Licensing.....	30
4.1.1.	SIP Trunk Capacity Check	30
4.1.2.	AAR/ARS Routing Check	30
4.1.3.	Configure Trunk-to-Trunk Transfers	30
4.2.	Configure Codec Type.....	30
4.3.	Set IP Network Region	31
4.4.	Add Node Names and IP Addresses	31
4.5.	Configure SIP Signaling Group and Trunk Group.....	32
4.5.1.	Create a Signaling Group for SIP Trunk to Avaya Aura™ Session Manager ...	32
4.5.2.	Add a SIP Trunk Group to Connect to Avaya Aura™ Session Manager	33
4.6.	Configure Route Pattern.....	34
4.7.	Administer Numbering Plan	34
4.7.1.	Administer Uniform Dialplan	34
4.7.2.	Administer AAR analysis	35
5.	Verification Steps.....	36
5.1.	Verify Avaya Aura™ Session Manager Configuration.....	36
5.1.1.	Verify Avaya Aura™ Session Manager is Operational	36
5.1.2.	Verify SIP Link Status.....	38
5.1.3.	Verify Registrations of SIP Endpoints.....	39
5.2.	Verify Avaya Aura™ Communication Manager Feature Server Configuration.....	40
5.3.	Call Scenarios Verified	42
6.	Acronyms.....	43
7.	Conclusion.....	44
8.	Additional References.....	44

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to support registration of 9600-Series SIP phones and enables connectivity to an Avaya Aura™ Communication Manager Feature Server 5.2.1 using SIP trunks.

As shown in **Figure 1**, Avaya Aura™ Session Manager is managed by Avaya Aura™ System Manager. Avaya 9620 IP Telephones configured as SIP endpoints utilize the Avaya Aura™ Session Manager User Registration feature and require an Avaya Aura™ Communication Manager operating as a Feature Server. Communication Manager Feature Server only supports IP Multimedia Subsystem (IMS)-SIP users that are registered to Avaya Aura™ Session Manager. The Communication Manager Feature Server is connected to Session Manager via an IMS-enabled SIP signaling group and associated SIP trunk group.

The Avaya 9600-Series IP Telephone (H.323) and 2420 Digital Telephone are supported by Avaya Aura™ Communication Manager Access Element. The Communication Manager Access Element is connected over a SIP trunk to the Avaya Aura™ Session Manager, using its SM-100 (Security Module) network interface. All inter-system calls are carried over these SIP trunks.

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8510 Server, Avaya Aura™ Communication Manager 5.2.1 Feature Server runs on a S8300 Server with Avaya G450 Media Gateway, and Avaya Aura™ Communication Manager 5.2.1 Access Element runs on an Avaya S8730 Server with Avaya G650 Media Gateway. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager 5.2.1.

These Application Notes will focus on the configuration of the Communication Manager Feature Server and Session Manager. Detailed administration of Communication Manager Access Element will not be described (see the appropriate documentation listed in **Section 8**).

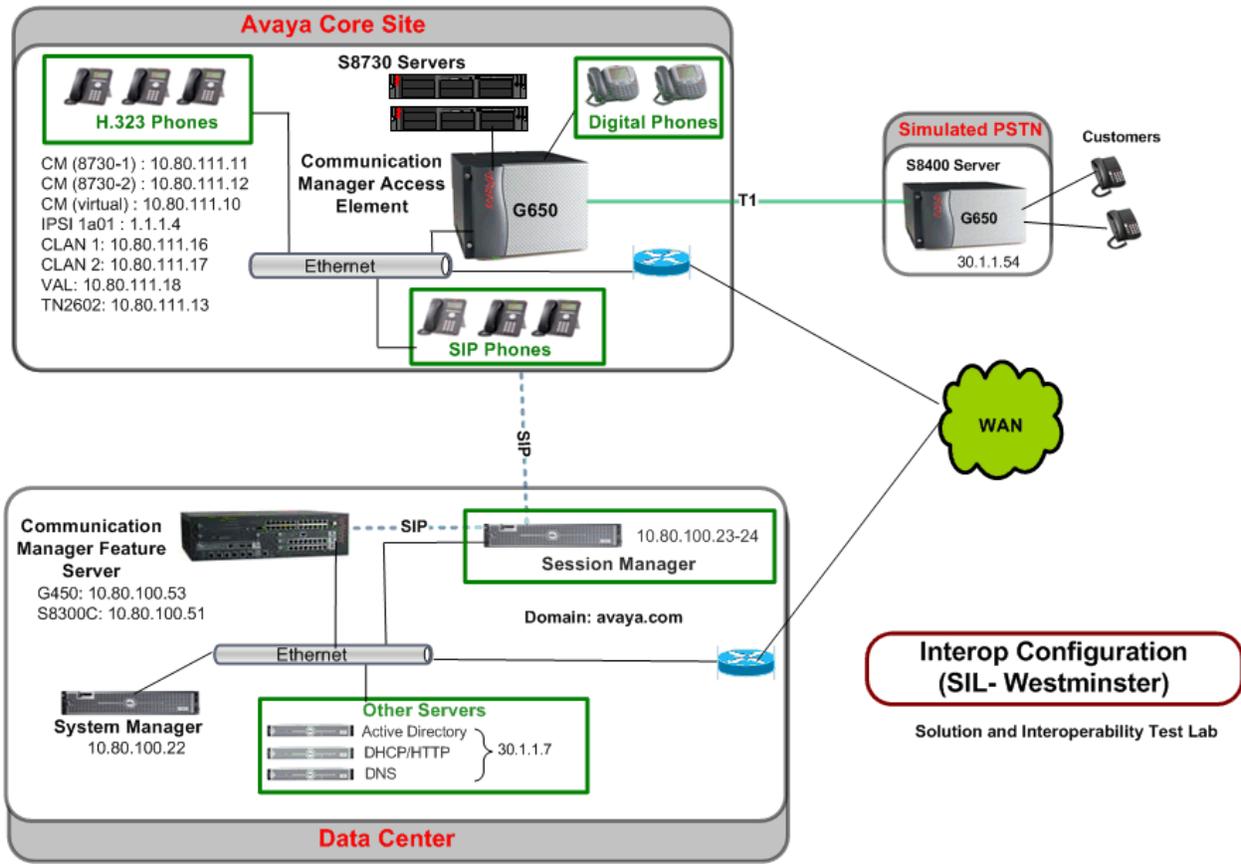


Figure 1 – Sample Configuration

1.1. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Equipment	Software
Avaya Aura™ Session Manager	Release 5.2.0.1.520017-11-18-2009
Avaya Aura™ System Manager	Release 5.2, Load: 5.2.0.8.27
Avaya Aura™ Communication Manager • Avaya S8730 Server Access Element	5.2.1 R015x.02.1.016.4
Avaya Aura™ Communication Manager • Avaya S8300 Feature Server	5.2.1 R015x.02.1.016.4
Avaya IP Telephones (H.323): • 9650 • 9630 • 9620	FW: 2.0 FW: 3.0 FW:1.5
Avaya SIP Phones • 9630	FW: 2.5.5.16
Avaya Digital Telephones (8410D)	N/A

2. Configuring Avaya Aura™ Communication Manager Feature Server

This section describes the administration of Communication Manager Feature Server using a System Access Terminal (SAT). Alternatively, some of the station administration could be performed using the Communication System Management application on System Manager. These instructions assume the G450 Media Gateway is already configured on the Communication Manager Feature Server. Some administration screens have been abbreviated for clarity.

- Verify System Capabilities and Communication Manager Licensing
- Administer network region
- Administer IP node names
- Administer IP interface
- Administer SIP trunk group and signaling group
- Administer route patterns
- Administer numbering plan

After completing these steps, the “**save translations**” command should be performed.

2.1. Verify System Capabilities and Licensing

This section describes the procedures to verify the correct system capabilities and licensing have been configured. If there is insufficient capacity or a required feature is not available, contact an authorized Avaya sales representative to make the appropriate changes.

2.1.1. SIP Trunk Capacity Check

Issue the **display system-parameters customer-options** command to verify that an adequate number of SIP trunk members are licensed for the system as shown below:

<code>display system-parameters customer-options</code>	Page	2 of	11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	500	0	
Maximum Concurrently Registered IP Stations:	18000	4	
Maximum Administered Remote Office Trunks:	0	0	
Maximum Concurrently Registered Remote Office Stations:	0	0	
Maximum Concurrently Registered IP eCons:	0	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	0	0	
Maximum Video Capable IP Softphones:	0	0	
Maximum Administered SIP Trunks:	50	20	

2.1.2. AAR/ARS Routing Check

Verify that **ARS** and **ARS/AAR Dialing without FAC** are enabled (on page 3 of system-parameters customer options).

```

display system-parameters customer-options                               Page 3 of 11
                                OPTIONAL FEATURES

A/D Grp/Sys List Dialing Start at 01? n                               CAS Main? n
Answer Supervision by Call Classifier? n                               Change COR by FAC? n
                                ARS? y Computer Telephony Adjunct Links? y
                                ARS/AAR Partitioning? y Cvg Of Calls Redirected Off-net? y
                                ARS/AAR Dialing without FAC? y DCS (Basic)? y
                                ASAI Link Core Capabilities? y DCS Call Coverage?

```

2.1.3. Configure Trunk-to-Trunk Transfers

Use the “**change system-parameters features**” command to enable trunk-to-trunk transfers. This feature is needed to be able to transfer an incoming/outgoing call from/to the remote switch back out to the same or another switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution.

```

change system-parameters features                                       Page 1 of 18
                                FEATURE-RELATED SYSTEM PARAMETERS
                                Self Station Display Enabled? n
                                Trunk-to-Trunk Transfer: all
                                Automatic Callback with Called Party Queuing? n
                                Automatic Callback - No Answer Timeout Interval (rings): 3

```

2.1.4. Enable Private Numbering

Use the “**change system-parameters customer-options**” command to verify that Private Networking is enabled as shown below:

```

display system-parameters customer-options                               Page 5 of 11
                                OPTIONAL FEATURES

Multinational Locations? y                Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n  Station as Virtual Extension? y
    Multiple Locations? y
Personal Station Access (PSA)? y          System Management Data Transfer? n
    PNC Duplication? n                    Tenant Partitioning? n
    Port Network Support? n               Terminal Trans. Init. (TTI)? y
    Posted Messages? n                    Time of Day Routing? n
                                           TN2501 VAL Maximum Capacity? y
                                           Uniform Dialing Plan? y
                                           Usage Allocation Enhancements? y

    Private Networking? y
Processor and System MSP? y
Processor Ethernet? y
                                           Wideband Switching? n
                                           Wireless? y

```

2.2. Add Node Name of Avaya Aura™ Session Manager

Using the **change node-names ip** command, add the node-name and IP for the Session Manager, if not previously added.

```

change node-names ip                                                  Page 1 of 2
                                IP NODE NAMES
Name                          IP Address
ASM1                        10.80.100.24
Nortel-CS1000e                10.80.50.50
default                        0.0.0.0
procr                       10.80.100.51

```

2.3. Configure IP Network Region

Using the **change ip-network-region 1** command, set the **Authoritative Domain** to the correct SIP domain for the configuration. Verify the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields are set to “yes”.

```

change ip-network-region 1                                           Page 1 of 19
                                IP NETWORK REGION
Region: 1
Location: 1                Authoritative Domain: avaya.com
Name:
MEDIA PARAMETERS
    Codec Set: 1                Intra-region IP-IP Direct Audio: yes
    UDP Port Min: 2048          Inter-region IP-IP Direct Audio: yes
    UDP Port Max: 16585        IP Audio Hairpinning? n

```

2.4. Add SIP Signaling Group

Issue the **add signaling-group n** command, where “n” is an available signaling group number, for one of the SIP trunks to the Session Manager, and fill in the indicated fields.

In the sample configuration, trunk group “10” and signaling group “10” were used to connect to Avaya Aura™ Session Manager. Default values can be used for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tcp”¹
- **IMS Enabled?:** “y”
- **Near-end Node Name:** procr from **Section 2.2**
- **Far-end Node Name:** Session Manager node name from **Section 2.2**
- **Near-end Listen Port:** “5060”
- **Far-end Listen Port:** “5060”
- **Far-end Domain:** Authoritative Domain from **Section 2.3**
- **Enable Layer 3 Test:** “y”
- **Session Establishment Timer:** “3”²

```

display signaling-group 10                                     Page 1 of 1
                                                           SIGNALING GROUP

Group Number: 10                                           Group Type: sip
                                                           Transport Method: tcp

  IMS Enabled? y
    IP Video? n

  Near-end Node Name: procr                               Far-end Node Name: ASM1
Near-end Listen Port: 5060                               Far-end Listen Port: 5060
                                                           Far-end Network Region: 1

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate                     Bypass If IP Threshold Exceeded? n
    DTMF over IP: rtp-payload                             RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3                       Direct IP-IP Audio Connections? y
    Enable Layer 3 Test? y                                IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n                   Direct IP-IP Early Media? n
                                                           Alternate Route Timer(sec): 6
  
```

2.5. Add SIP Trunk Group

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where “n” is an available trunk group number and fill in the indicated fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”

¹ TCP was used for the sample configuration. However, TLS would typically be used in production environments.

² If any call originating from the SIP phone is not expected to be answered within 3 minutes such would happen if the call is made to a VDN and agents are not available within 3 minutes, this value may need to be increased.

- **Signaling Group:** The number of the signaling group added in **Section 2.4**
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total number of trunks configured in **Section 2.1.1**).

```

add trunk-group 10                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 10                                     Group Type: sip          CDR Reports: y
  Group Name: ASM1                                   COR: 1                  TN: 1          TAC: #10
Direction: two-way                                  Outgoing Display? n
Dial Access? n                                       Night Service:
Queue Length: 0
Service Type: tie                                     Auth Code? n
                                                    Signaling Group: 10
                                                    Number of Members: 10

```

Once the add command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

On page 2, set the **Preferred Minimum Session Refresh Interval** to 1200. Note: to avoid extra SIP messages, all SIP trunks connected to Session Manager should be configured with a minimum value of 1200.

```

add trunk-group 10                                     Page 2 of 21
                                     Group Type: sip
TRUNK PARAMETERS
Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
SCCAN? n                                           Digital Loss Group: 18
                                     Preferred Minimum Session Refresh Interval(sec): 1200

```

On page 3, set **Numbering Format** to be *private*. Use default values for all other fields.

```

add trunk-group 10                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                   Measured: none
                                                    Maintenance Tests? y

  Numbering Format: private
                                                    UUI Treatment: service-provider
                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n
  
```

2.6. Administering Numbering Plan

SIP Users registered to Session Manager need to be added to either the private or public numbering table on the Communication Manager Feature Server. For the sample configuration, private numbering was used and all extension numbers were unique within the private network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in References [3] and [8].

To enable SIP endpoints to dial extensions defined in the Communication Manager Access Element, use the “**change private-numbering x**” command, where x is the number used to identify the private number plan. For the sample configuration, extension numbers starting with 5XX-XXXX or 6XX-XXX are used on the Communication Manager Access Element.

- **Ext Len:** Enter the extension length allowed by the dial plan
- **Ext Code:** Enter leading digit (s) from extension number
- **Trunk Grp:** Enter the SIP Trunk Group number for the SIP trunk between the Feature Server and Session Manager
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.

```

change private-numbering 1                             Page 1 of 2
                                                    NUMBERING - PRIVATE FORMAT

Ext  Ext      Trk      Private      Total
Len  Code     Grp(s)    Prefix       Len
 7   5         10        7            7      Total Administered: 2
 7   6         10        7            7      Maximum Entries: 540
  
```

2.7. Configure Stations

For each SIP user to be defined in Session Manager, add a corresponding station on the Communication Manager Feature Server. Note: instead of manually defining each station using the Communication Manager SAT interface, an alternative option is to automatically generate the SIP station when adding a new SIP user. See Section 3.4.6 for more information on adding SIP users.

The phone number defined for the station will be the number the SIP user enters to register to Session Manager. Use the “**add station x**” command where x is a valid extension number defined in the system. On page 1 of the change station form:

- **Phone Type:** Set to 96xxSIP
- **Name:** Display name for user
- **Security Code:** number used when user logs into station. Note: this code should match the “**Shared Communication Profile Password**” field defined when adding this user in Session Manager. See **Section 3.4.5**.

```
add station 6663000                                     Page 1 of 6
                                     STATION
Extension: 666-3000                               Lock Messages? n          BCC: 0
Type: 9630SIP                                     Security Code: 123456   TN: 1
Port: S00006                                         Coverage Path 1: 1       COR: 1
Name: John Smith                                  Coverage Path 2:         COS: 1
                                                         Hunt-to Station:
STATION OPTIONS
                                     Time of Day Lock Table:
Loss Group: 19
Display Language: english
Survivable COR: internal
Survivable Trunk Dest? y
                                     Message Lamp Ext: 666-3000
                                     Button Modules: 0
                                     IP SoftPhone? n
                                     IP Video? n
```

On page 6, set:

- **SIP Trunk option:** Enter SIP Trunk Group defined in **Section 2.5**

```
change station 6663000                                 Page 6 of 6
                                     STATION
SIP FEATURE OPTIONS
Type of 3PCC Enabled: None
SIP Trunk: 10
```

Note: an alternative option for configuring stations is to use the option when adding a SIP user in Session Manager to automatically generate the station. See Section 3.4.5 for more information on using Session Manager to add SIP users.

2.8. Configure Off-PBX-Telephone Station-Mapping

Use the “**change off-pbx-telephone station-mapping**” command for each extension associated with SIP users defined in Session Manager. On page 1, enter the SIP Trunk Group defined in Section 2.5 and use default values for other fields.

```
change off-pbx-telephone station-mapping 6663000 Page 1 of 3
```

STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
666-3000	OPS	-	-	6663000	10	1	
		-	-				
		-	-				

On page 2, enter the following values:

- **Mapping Mode:** “both”
- **Calls Allowed:** “all”

```
change off-pbx-telephone station-mapping 6663000 Page 2 of 3
```

STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station Extension	Appl Name	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location
666-3000	OPS	3	both	all	none	

2.9. Save Translations

Configuration of Communication Manager Feature Server is complete. Use the “**save translations**” command to save these changes

Note: After a change on Communication Manager Feature Server which alters the dial plan, synchronization between Communication Manager Feature Server and Session Manager needs to be completed and SIP phones must be re-registered. To request an on demand synchronization, log into the System Manager console and use the **Synchronize CM Data** feature under the Communication System Management menu.

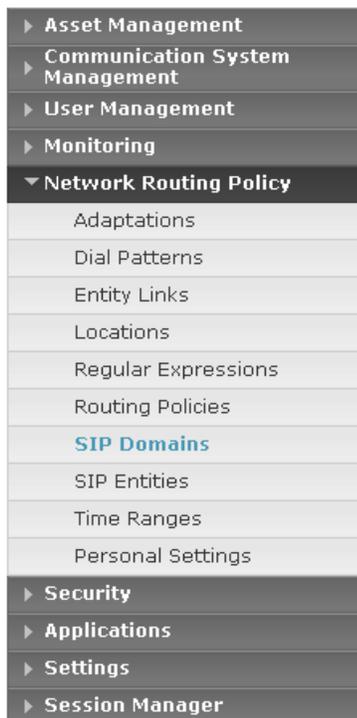
3. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring the Session Manager and includes the following items:

- Administer SIP domain
- Define Logical/physical Locations that can be occupied by SIP Entities
- For each SIP entity in the sample configuration:
 - Define SIP Entity
 - Define Entity Links, which define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from SIP Entities
 - Define Routing Policies, which control call routing between the SIP Entities
 - Define Dial Patterns, which govern to which SIP Entity a call is routed
- Define the Communication Manager Feature Server as an administration entity
- Adding SIP Endpoints/SIP URE users

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura™ System Manager, using the URL “http://<ip-address>/SMGR”, where “<ip-address>” is the IP address of Avaya Aura™ System Manager.

Log in with the appropriate credentials and accept the Copyright Notice. Expand the **Network Routing Policy** Link on the left side of Navigation Menu. Select a specific item such as SIP Domains. When the specific item is selected, the color of the item will change to blue as shown below:



3.1. Administer SIP Domains

- Expand Network Routing Policy and select **SIP Domains**.
 - Click **New**
 - In the *General* Section, under *Name* add a descriptive name. Under *Notes* add a brief description.
 - Click **Commit** to save.

The screen below shows the information for the sample configuration.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name, and a user status message: "Welcome, admin Last Logged on at Jan. 04, 2010 12:56 PM". A breadcrumb trail shows "Home / Network Routing Policy / SIP Domains". On the left, a sidebar menu lists various management categories, with "Network Routing Policy" expanded to show "SIP Domains" selected. The main content area, titled "Domain Management", features action buttons for "Edit", "New", "Duplicate", "Delete", and "More Actions". Below these is a table with one item, "avaya.com", which is a "sip" domain. The table has columns for "Name", "Type", "Default", and "Notes". A "Filter: Enable" option is visible in the top right of the table area. Below the table, a selection status indicates "Select : All, None (0 of 1 Selected)".

3.2. Define Locations

- Expand Network Routing Policy and select **Locations**. Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.
 - Click **New**
 - In the *General* Section, under *Name* add a descriptive name.
 - Under *Notes* add a brief description.
 - In the *Location Pattern* Section, under IP Address Pattern enter pattern used to logically identify the location Under *Notes* add a brief description.
 - Click **Commit** to save.

The screen below shows the information for Communication Manager Access Element in the sample configuration.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Jan. 04, 2010 1:38 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Locations / Location Details

Location Details

General

* Name:
 Notes:

Managed Bandwidth:
 * Average Bandwidth per Call: Kbit/sec
 * Time to Live (secs):

Location Pattern

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.80.111.*	<input type="text"/>

Select : All, None (0 of 1 Selected)

Shortcuts

* Input Required

3.3. Add Avaya Aura™ Communication Manager Access Element

3.3.1. Define SIP Entity for the Avaya Aura™ Communication Manager Access Element

- Expand Network Routing Policy
 - Select SIP Entities
 - Click **New**
 - In the *General* Section, under *Name* add an identifier for the Communication Manager. Under *FQDN or IP Address* enter the IP Address of the Communication Manager. Under *Type* select CM. Under *Notes* add a brief description.
 - *Location*: From the drop-down select the Location added in **Section 3.2**. Note: since location-based routing was not used in the sample configuration, selecting a value for location field is optional.
 - Click **Commit** to save.

The following screen shows addition of Communication Manager Access Element. The IP address used is that of the C-LAN board in the Avaya G650 Media Gateway.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 04, 2010 3:33 PM
Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

SIP Entity Details Commit Cancel

General

* Name: S8730-2

* FQDN or IP Address: 10.80.111.17

Type: CM

Notes: S8730 Pair - CLAN-2

Adaptation: [Dropdown]

Location: [Dropdown]

Time Zone: America/Denver

Override Port & Transport with DNS SRV:

* SIP Timer B/F (in seconds): 4

Credential name: [Text Field]

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

1 Item Refresh Filter: Enable						
<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	ASM1-DR	TCP	* 5060	S8730-2	* 5060	<input checked="" type="checkbox"/>

Select : All, None (0 of 1 Selected)

* Input Required Commit Cancel

3.3.2. Define an Entity Link for Avaya Aura™ Communication Manager Access Element

- Expand Network Routing Policy
 - Entity Links
 - Click **New**
 - Under *Name*, enter an identifier for the Communication Manager Access Element.
 - Under *SIP Entity 1* drop-down select the appropriate Session Manager. Under *Port* drop-down select the correct port for the Session Manager.
 - Under *SIP Entity 2* drop-down select the SIP Entity added in **Section 3.3.1** for the Communication Manager Access Element. Under *Port* drop-down select the correct port for the Communication Manager. Select it as a *Trusted* host. Under *Protocol* drop-down select the required protocol.
 - Under *Notes* add a brief description.

- Click **Commit** to save.

The following screen shows the entity link defined for the Communication Manager Access Element.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 04, 2010 3:33 PM Help | Log off

Home / Network Routing Policy / Entity Links

Entity Links Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ADM1 to S8730-2	* ASM1-DR	TCP	* 5060	* S8730-2	* 5060	<input checked="" type="checkbox"/>	

* Input Required Commit Cancel

3.3.3. Define Routing Policy for Avaya Aura™ Communication Manager Access Element

- Expand Network Routing Policy
 - Routing Policies
 - Click **New**
 - In the 'General' section, under Name add an identifier to define the routing policy for the Communication Manager. Under *Notes* add a brief description.
 - In the 'SIP Entity as Destination' section, click on **Select**.
 - The SIP Entity List page opens.
 - Select the entry of the Communication Manager added in **Section 3.3.1** and click on **Select**
 - The selected SIP Entity displays on the Routing Policy Details page.
 - Click on **Commit** to save.

Shown below is the updated screen for the sample configuration which includes the list of dial patterns for any extension numbers that SIP users will dial to reach stations on the Communication Manager Access Element.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Jan. 04, 2010 3:33 PM
Help | Log off

Home / Network Routing Policy / Routing Policies / Routing Policy Details

Routing Policy Details Commit Cancel

General

* Name:
 Disabled:
 Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
S8730-1	10.80.111.16	CM	S8730 Pair CLAN-1

Time of Day

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7						

Select : All, None (0 of 1 Selected)

Dial Patterns

5 Items Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	400	7	7	<input type="checkbox"/>	-ALL-	-ALL-	
<input type="checkbox"/>	5221	7	7	<input type="checkbox"/>	-ALL-	-ALL-	to S8730 Agents
<input type="checkbox"/>	5223	7	7	<input type="checkbox"/>	-ALL-	-ALL-	direct call to VP VDN on S8730
<input type="checkbox"/>	6661	7	7	<input type="checkbox"/>	-ALL-	-ALL-	
<input type="checkbox"/>	6664	7	7	<input type="checkbox"/>	-ALL-	-ALL-	to S8730 CM

Select : All, None (0 of 5 Selected)

3.3.4. Define Dial Plan for calls to Avaya Aura™ Communication Manager Access Element

- Expand Network Routing Policy
 - Dial Patterns
 - Click **New**
 - In the 'General' section, under *Pattern* add the numbers that SIP users will dial to reach other extensions on the Communication Manager Access Element. Under *Min* enter the minimum number digits that must be dialed. Under *Max* enter the maximum number digits that may be dialed.
 - Under SIP Domain drop-down, select the SIP Domain added in **Section 3.1** or select "All" if the system can accept incoming call from all SIP domains.
 - Under *Notes* add a brief description.

- In the 'Originating Locations and Routing Policies' section click on **Add**
 - The 'Locations and Routing Policy List' page opens.
 - Under Locations, select the desired location.
- Under Routing Policies, select the one defined for Communication Manager in **Section 3.3.2** and click on **Select**.

Shown below is the updated screen for one of the dial patterns in the sample configuration.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 04, 2010 1:38 PM
Help | Log off

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

Dial Pattern Details Commit Cancel

General

* Pattern: 6654
 * Min: 7
 * Max: 7
 Emergency Call:
 SIP Domain: -ALL-
 Notes: to S8730 CM

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to S8730 CM	0	<input type="checkbox"/>	S8730-1	

Select : All, None (0 of 1 Selected)

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
<input type="checkbox"/>		

* Input Required Commit Cancel

3.4. Add Avaya Aura™ Communication Manager Feature Server

The following section captures relevant screens for configuring Avaya Aura™ Communication Manager Feature Server applicable for the sample configuration.

3.4.1. Define a SIP Entity for Avaya Aura™ Communication Manager Feature Server

The following screen shows addition of Communication Manager Feature Server. The IP address used is that of the S8300C server.



- Asset Management
- Communication System Management
- User Management
- Monitoring
- Network Routing Policy**
 - Adaptations
 - Dial Patterns
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities**
 - Time Ranges
 - Personal Settings
- Security
- Applications
- Settings
- Session Manager

- Shortcuts**
- Change Password
 - Help for SIP Entity Details fields
 - Help for Committing configuration changes

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV:

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

* Proactive Monitoring Interval (in seconds):

* Reactive Monitoring Interval (in seconds):

* Number of Retries:

Entity Links

1 Item Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	ASM1-DR	TCP	* 5060	S8300-G450-FS	* 5060	<input checked="" type="checkbox"/>

Select : All, None (0 of 1 Selected)

* Input Required

3.4.2. Define Entity Link for Avaya Aura™ Communication Manager Feature Server

The following screen shows the entity link defined for the Avaya Aura™ Communication Manager Feature Server.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Jan. 04, 2010 12:56 PM
Help | Log off

Home / Network Routing Policy / Entity Links

Entity Links Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
*ASM-to-S8300-2	*ASM1-DR	TCP	*5060	*S8300-G450-FS	*5060	<input checked="" type="checkbox"/>	

* Input Required Commit Cancel

3.4.3. Define Routing Policy for Avaya Aura™ Communication Manager Feature Server

Since the SIP users are registered on Session Manager, a routing policy does not need to be defined for the Communication Manager Feature Server.

3.4.4. Define Application Sequence for Avaya Aura™ Communication Manager Feature Server

Define an application for the Avaya Aura™ Communication Manager Feature Server as shown below:

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar is red and contains the Avaya logo, the text "Avaya Aura™ System Manager 5.2", and a user status "Welcome, admin Last Logged on at Jan. 04, 2010 1:38 PM" with a "Help Log off" link. Below the navigation bar is a breadcrumb trail: "Home / Session Manager / Application Configuration / Application Editor".

The main content area is titled "Application Editor" and includes a "Commit" and "Cancel" button. The "Application Editor" section contains the following fields:

- Name:** S8300-G450-APP
- * SIP Entity:** S8300-G450-FS (dropdown menu)
- Description:** CM as FS only

Below these fields is the "Application Attributes (optional)" section, which contains a table with two columns: "Name" and "Value".

Name	Value
Application Handle	<input type="text"/>
URI Parameters	<input type="text"/>

At the bottom of the "Application Attributes" section, there is a "* Required" label and another "Commit" and "Cancel" button.

Second, define an application sequence for the Avaya Aura™ Communication Manager Feature Server as shown below:

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 04, 2010 1:38 PM
Help Log off

Home / Session Manager / Application Configuration / Application Sequence Editor

Application Sequence Editor Commit Cancel

Sequence Name

Name:
 Description:

Applications in this Sequence

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		S8300-G450-APP	S8300-G450-FS	<input checked="" type="checkbox"/>	CM as FS only

Select : All, None (0 of 1 Selected)

Available Applications

2 Items Refresh Filter: Enable

	Name	SIP Entity	Description
+	S8300-G450-APP	S8300-G450-FS	CM as FS only
+	Voice Portal	VPMS	VPMS/MPP Server running VP app

*Required Commit Cancel

3.4.5. Define Avaya Aura™ Communication Manager Feature as an Administrable Entity

Before adding SIP users, the Avaya Aura™ Communication Manager Feature Server must also be added to System Manager as an administrable entity. This action allows System Manager to access Communication Manager over its administration interface similar to how other administration tools such as Avaya Site Administrator access Communication Manager. Using this administration interface, System Manager will notify the Communication Manager Feature Server when new SIP users are added.

To define the Avaya Aura™ Communication Manager Feature Server as an administrable entity,

- Expand Applications
 - Entities -> Applications
 - Click **New**
 - Under *Name*, enter an identifier for the Communication Manager Feature Server.
 - Under *Type* drop-down menu, select CM.
 - Under *Node*, enter the IP address of the administration interface for the Feature Server as shown below:

- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▼ Applications
 - FPM
 - MSA
 - NMC
 - Session Manager 5.2
 - SMGR
 - SIP AS 8.0
 - Entities
- ▶ Settings
- ▶ Session Manager

Shortcuts

Edit CM: S8300-G450

Application | Port | Access Point | Attributes |
 Expand All | Collapse All

Application ▼

* Name

* Type

Description

* Node

Port ▶

Access Point ▶

Defining the Avaya Aura™ Communication Manager Feature Server as an administrable entity (continued):

o Entities - Attributes

- Under *Login and Password*, enter the login and password used for administration access to the Feature Server.
- Select SSH access.
- Under *Port*, enter the port number for the administration interface of 5022 as shown below:

Attributes ▼

* Login

Password

Confirm Password

Is SSH Connection

* Port

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Alternate IP Address

Is ASG Enabled

ASG Key

Confirm ASG Key

Location

*Required

Defining the Avaya Aura™ Communication Manager Feature Server as an administrable entity (continued):

- Entities – Port
- Entities – Access Point

Although the port number for the administration interface is defined under the Attribute tab, no additional data is needed for either the Port or Access Point tabs as shown below:

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura™ System Manager 5.2', and a user status 'Welcome, admin Last Logged on at Jan. 04, 2010 12:56 PM'. Below the navigation bar is a breadcrumb trail: 'Home / Applications / Application Management / Applications Details'. The left sidebar contains a menu with categories like 'Asset Management', 'Communication System Management', 'User Management', 'Monitoring', 'Network Routing Policy', 'Security', 'Applications', 'Settings', and 'Session Manager'. The 'Applications' category is expanded, showing sub-items like 'FPM', 'MSA', 'NMC', 'Session Manager 5.2', 'SMGR', 'SIP AS 8.0', and 'Entities'. Below the sidebar is a 'Shortcuts' section with a 'Change Password' link. The main content area is titled 'Edit CM: S8300-G450' and includes 'Commit' and 'Cancel' buttons. It features a navigation bar with 'Application | Port | Access Point | Attributes' and 'Expand All | Collapse All' options. The 'Application' tab is active, showing fields for '* Name' (S8300-G450), '* Type' (CM), 'Description' (CM5.2.1), and '* Node' (10.80.100.51). Below this are sections for 'Port' and 'Access Point', each with 'View', 'Edit', 'New', and 'Delete' buttons. Both sections show a table with 0 items and the message 'No records found.'.

3.4.6. Add SIP Users

Add SIP users corresponding to the 96XX SIP stations defined in **Section 2.7**. Alternatively, use the option to automatically generate the SIP stations on Communication Manager Feature Server when adding a new SIP user.

- Expand User Management
 - Select User Management
 - Click **New**

Step 1: Enter values for the following required attributes for a new SIP user in the **General** and **Identity** sections of the new user form.

- **Last Name:** enter last name of user
- **First Name:** enter first name of user
- **Login Name:** enter extension no. @sip domain defined in **Section 3.1**. This field is primary handle of user.
- **Authentication Type:** select **Basic**
- **SMGR Login Password:** enter password which will be used to log into System Manager application
- **Confirm Password:** repeat value entered above
- **Shared Communication Profile Password:** enter a numeric value which will be used to logon to SIP phone. *Note:* this field must match the Security Code field on the station form defined in **Section 2.7**.
- **Confirm Password:** repeat numeric password

The screen below shows the information when adding a new SIP user to the sample configuration.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 04, 2010 1:38 PM
Help | Log off

Home / User Management / User Management / New User

New User Profile Commit Cancel

General | Identity | Communication Profile | Roles | Override Permissions | Group Membership | Attribute Sets | Default Contact List | Private Contacts |
Expand All | Collapse All

General

* Last Name: Doe

* First Name: Jane

Middle Name:

Description:

administrator
 communication_user
 agent

User Type: supervisor
 resident_expert
 service_technician
 lobby_phone

Identity

* Login Name: 663002@avaya.com

* Authentication Type: Basic

SMGR Login Password:

* Password:

* Confirm Password:

Shared Communication Profile Password:

Confirm Password:

Localized Display Name: Jane Doe

Step 2: Scroll down to the Communication Profile section and select **New** to define a **Communication Profile** for the new SIP user. Enter values for the following required attributes:

- **Name:** enter name of communication profile
- **Default:** enter checkmark to indicate this profile is default profile

Select **New** to define a **Communication Address** for the new SIP user. Enter values for the following required attributes:

- **Type:** select SIP
- **SubType:** select username
- **Handle:** enter extension number
- **Domain:** enter SIP domain defined in **Section 3.1**

The screen below shows the information when adding a new SIP user to the sample configuration.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 04, 2010 1:38 PM
Help | Log off

Home / User Management / User Management / **New User**

New User Profile Commit Cancel

General | Identity | Communication Profile | Roles | Override Permissions | Group Membership | Attribute Sets | Default Contact List | Private Contacts | Expand All | Collapse All

General ▾

Identity ▾

Communication Profile ▾

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary

Default:

Communication Address ▾

New Edit Delete

<input type="checkbox"/>	Type	SubType	Handle	Domain
<input type="checkbox"/>	sip	username	6663002	avaya.com

Select : All, None (0 of 1 Selected)

Step 3: Assign the **Application Sequence** defined in **Section 3.4.4** to the new SIP user as part of defining the **SIP Communication Profile**. The **Application Sequence** can be used for both the originating and terminating sequence. Enter values for the following required attributes of the **Station Profile** section:

- **System:** select the SIP Entity of the Communication Manager Feature Server defined in **Section 3.4.1** from menu

- **Use Existing Stations:** enter checkmark if station was already defined. Else, station will automatically be created.
- **Extension:** enter extension number
- **Template:** select template for type of SIP phone
- **Security Code:** enter numeric value which will be used to logon to SIP phone.
Note: this field must match the value entered for the **Shared Communication Profile Password** field
- **Port:** select port number from the list for the selected template
- **Delete Station on Unassign of Station:** enter checkmark to automatically delete station when **Station Profile** is un-assigned from user.

The screen below shows the information when adding a new SIP user to the sample configuration.

Communication Profile ▾

New Delete Done Cancel

Name
Primary
Select : None

* Name: Primary

Default:

Communication Address ▶

Session Manager ▾

* Session Manager Instance ASM1-DR ▾

Origination Application Sequence CM App Seq 1 ▾

Termination Application Sequence CM App Seq 1 ▾

Messaging Profile ▶

Station Profile ▾

* System S8300-G450 ▾

Use Existing Stations

* Extension 6663002

* Template DEFAULT_9630SIP ▾

Set Type 9630SIP

Security Code 123456

* Port S0007

Delete Station on Unassign of Station from User

4. Configuring Avaya Aura™ Communication Manager Access Element

This section describes the administration of Communication Manager Access Element using a System Access Terminal (SAT). Some administrative screens are not shown in this section, as they might be similar to **Section 2**.

- Verify System Capabilities and Communication Manager Licensing
- Administer IP network region
- Administer IP node names
- Administer SIP trunk group and signaling group
- Administer route patterns
- Administer numbering plan

After completing these steps, the “**save translations**” command should be performed.

4.1. Verify System Capabilities and Licensing

This section describes the procedures to verify the correct system capabilities and licensing have been configured. If there is insufficient capacity or a required feature is not available, contact an authorized Avaya sales representative to make the appropriate changes.

4.1.1. SIP Trunk Capacity Check

Use the “**display system-parameters customer-options**” command to verify that an adequate number of SIP trunk members are administered for the system. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

4.1.2. AAR/ARS Routing Check

Verify that **ARS** is enabled (on page 3 of system-parameters customer options).

4.1.3. Configure Trunk-to-Trunk Transfers

Use the “**change system-parameters features**” command to enable trunk-to-trunk transfers.

4.2. Configure Codec Type

Issue the **change ip-codec-set n** command where **n** is the next available number. Enter the following values:

- Enter “**G.711MU**” and “**G.729**” as supported types of Audio Codecs
- Silence Suppression: Retain the default value “**n**”.

- Frames Per Pkt: Enter “2”.
- Packet Size (ms): Enter “20”.
- Media Encryption: Enter the value based on the system requirement. For the sample configuration, “none” was used.

```
change ip-codec-set 1                                     Page 1 of 2
                                     IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G.711MU      n           2          20
2: G.729      n           2          20
3:

Media Encryption
1: none
```

4.3. Set IP Network Region

Using the **change ip-network-region 1** command, set the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields to “yes”. For the **Codec Set** enter the corresponding audio codec set configured in **Section 4.1**. Set the **Authoritative Domain** to the correct SIP domain for the configuration.

```
change ip-network-region 1                               Page 1 of 19
                                     IP NETWORK REGION

Region: 1
Location:      Authoritative Domain: avaya.com
Name:

MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 1          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 16585
```

4.4. Add Node Names and IP Addresses

Using the **change node-names ip** command, add the node-name and IP for the CLANs and the Session Manager, if not already previously added. Note the node names of the CLANs which will later be used to configure the SIP trunks between the Avaya G650 and the Session Manager.

```
change node-names ip                                     Page 1 of 2
                                     IP NODE NAMES

Name      IP Address
8730-1    10.80.111.11
8730-2    10.80.111.12
ASM1      10.80.100.24
ASM2      10.80.100.26
CLAN-1    10.80.111.16
CLAN-2    10.80.111.17
```

4.5. Configure SIP Signaling Group and Trunk Group

4.5.1. Create a Signaling Group for SIP Trunk to Avaya Aura™ Session Manager

Use the **add signaling-group n** command, where “n” is an available signaling group number to create a SIP trunk to the Session Manager. In the sample configuration, trunk group “10” and signaling group “10” were used to connect to Avaya Aura™ Session Manager. Fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tcp”³
- **IMS Enabled:** “n”
- **Near-end Node Name:** C-LAN node name from **Section 4.4**.
- **Far-end Node Name:** Session Manager node name from **Section 4.4**.
- **Near-end Listen Port:** “5060”
- **Far-end Listen Port:** “5060”
- **Far-end Domain:** enter domain name defined in IP Network Region for **Authoritative Domain** field. **See Section 4.3**
- **DTMF over IP:** “rtp-payload”
- **Session Establishment Timer:** “3”⁴

```
add signaling-group 10                                     Page 1 of 1
                                                         SIGNALING GROUP
Group Number: 10           Group Type: sip
                          Transport Method: tcp
  IMS Enabled? n
  IP Video? n
  Near-end Node Name: CLAN-2           Far-end Node Name: ASM1
  Near-end Listen Port: 5060           Far-end Listen Port: 5060
                                       Far-end Network Region:
Far-end Domain: avaya.com
                                       Bypass If IP Threshold Exceeded? n
  DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3    IP Audio Hairpinning? n
  Enable Layer 3 Test? n               Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

³ TCP was used for the sample configuration. However, TLS would typically be used in production environments.

⁴ If any call originating from the SIP phone is not expected to be answered within 3 minutes such would happen if the call is made to a VDN and agents are not available within 3 minutes, this value may need to be increased.

4.5.2. Add a SIP Trunk Group to Connect to Avaya Aura™ Session Manager

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where “n” is an available trunk group number and fill in the indicated fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Signaling Group:** The number of the signaling group added in **Section 4.5.1**
- **Number of Members:** The number of members in the SIP trunk to be allocated to calls routed to Session Manager (must be within the limits of the total number of trunks configured in **Section 4.1.1**).

Once the add command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

```
add trunk-group 10                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 10                                     Group Type: sip          CDR Reports: y
  Group Name: SIP trunk to ASM1                     COR: 1                  TN: 1          TAC: #10
Direction: two-way                                Outgoing Display? n
  Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                                  Auth Code? n
                                                    Signaling Group: 10
                                                    Number of Members: 10
```

On page 2, set the **Preferred Minimum Session Refresh Interval** to 1200. Note: to avoid extra SIP messages, all SIP trunks connected to Session Manager should be configured with a minimum value of 1200.

```
add trunk-group 10                                     Page 2 of 21
                                                    Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                                    Redirect On OPTIM Failure: 5000
  SCCAN? n                                          Digital Loss Group: 18
                                                    Preferred Minimum Session Refresh Interval(sec): 1200
```

On page 3, set **Numbering Format** to be *public*. Use default values for all other fields.

```
add trunk-group 10                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                   Measured: none
                                                    Maintenance Tests? y
  Numbering Format: public
                                                    UUI Treatment: service-provider
                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n
Show ANSWERED BY on Display? y
```

4.6. Configure Route Pattern

Use the “**add route-pattern X**” command, when **X** is an available number to define a route pattern for routing calls over the SIP trunk group defined in **Section 4.5** to Session Manager. In the sample configuration, route pattern 10 was created as shown below:

```
add route-pattern 10                                   Page 1 of 3
  Pattern Number: 10 Pattern Name: SIP to ASM1
  SCCAN? n      Secure SIP? n
  Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/ IXC
  No          Mrk Lmt List Del  Digits          QSIG
  Dgts
  1: 10  0
  2:
  3:                                     n user
                                     n user
                                     n user
```

4.7. Administer Numbering Plan

4.7.1. Administer Uniform Dialplan

Use the “**change uniform-dialplan x**” command, where **x** is the first digit of the extension numbers used for SIP stations in the system.

In the sample configuration, extensions starting with “666-3XXX” are used for extensions associated with the 96XX SIP phones.

```

change uniform-dialplan 6                                     Page 1 of 2
                                                           UNIFORM DIAL PLAN TABLE
                                                           Percent Full: 0
Matching
Pattern      Len Del      Insert      Node
              7  0      Digits      Net Conv Num
6663
6665000      7  0      aar n
777          7  0      aar n
778          7  0      aar n
              n
  
```

4.7.2. Administer AAR analysis

This section provides the configuration of the AAR pattern used in the sample configuration for routing calls between Communication Manager Access Element and SIP users registered to Session Manager.

Note that other methods of routing may be used.

Use the “**change aar analysis x**” command where **x** is the first digit of the extension numbers used for SIP stations in the system.

```

change aar analysis 6                                     Page 1 of 2
                                                           AAR DIGIT ANALYSIS TABLE
                                                           Location: all      Percent Full: 1
Dialed
String      Total      Route      Call      Node      ANI
              Min Max      Pattern      Type      Num      Reqd
6           7  7      10      aar      n
6663
6665000    7  7      20      aar      n
777        7  7      20      lev0     n
778        7  7      30      aar      n
8          7  7      999     aar      n
9          7  7      999     aar      n
  
```

5. Verification Steps

5.1. Verify Avaya Aura™ Session Manager Configuration

5.1.1. Verify Avaya Aura™ Session Manager is Operational

Verify the overall system status for the specific Session Manager as shown below:

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the system name "Avaya Aura™ System Manager 5.2", and a user status message: "Welcome, admin Last Logged on at Jan. 04, 2010 1:38 PM" with a "Help Log off" link. A red breadcrumb trail shows the path: Home / Session Manager / System Status / System State Administration.

The left sidebar contains a tree view of system components, with "System State Administration" selected under "System Status".

The main content area is titled "System State Administration" and includes a descriptive paragraph: "This page shows the current service and management state of configured Session Managers. You can use this page to make state changes in the context of an upgrade or necessary maintenance." Below this is a section for "Session Manager Instances" with three buttons: "Refresh", "Management State" (dropdown), and "Service State" (dropdown). A "Shutdown System" button is also present.

A table displays 2 items:

<input type="checkbox"/>	Session Manager	Management State	Service State	Last Service State Change	Active Call Count	Version
<input type="checkbox"/>	ASM1-DR	Management Enabled	Accept New Service	No last service state change	0	Development Patch on Version 5.2.0.0 05-Nov-09 14:55
<input type="checkbox"/>	ASM2-DR	Management Enabled	Accept New Service	Wed Nov 18 15:13:46 MST 2009	0	5.2.0.1.520017 - 11-18-2009

Below the table, it indicates "Select : All, None (0 of 2 Selected)".

Verify the status of the Security Module (SM 100 card) for the specific Session Manager as shown below:



- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ **Session Manager**
 - Session Manager Administration
 - ▶ Network Configuration
 - ▶ Device and Location Configuration
 - ▶ Application Configuration
 - ▼ **System Status**
 - System State Administration
 - SIP Entity Monitoring
 - Managed Bandwidth Usage
 - **Security Module Status**
 - Data Replication Status
 - RegistrationSummary
 - User Registrations
 - ▶ System Tools

- Shortcuts**
- [Change Password](#)
 - [Help for Security Module Status](#)
 - [Help for Page Fields](#)

Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

Security Module Statistics

Stat Name	ASM1-DR	ASM2-DR
Security Module Deployment	Up	Up
IP Address	10.80.100.24	10.80.100.26
Network Mask	255.255.255.0	255.255.255.0
Default Gateway	10.80.100.1	10.80.100.1
Interface Name	eth0	eth0
Name Servers	192.11.13.2	192.11.13.2
DNS Search	---	---
Call Control PHB	46	46
Speed & Duplex	Auto	Auto
VLAN	---	---
QOS	---	---
Certificate Used	Default Certificate (Issued By SIP CA)	Default Certificate (Issued By SIP CA)
Trusted Hosts (expected/actual)	8/8	0/0

Security Module Actions

System Name
<input type="radio"/> ASM1-DR
<input type="radio"/> ASM2-DR
Select : None

Finally, verify the data replication status is operational as shown below:



- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ **Session Manager**
 - Session Manager Administration
 - ▶ Network Configuration
 - ▶ Device and Location Configuration
 - ▶ Application Configuration
 - ▼ **System Status**
 - System State Administration
 - System State Monitoring
 - Managed Bandwidth Usage
 - Security Module Status
 - Data Replication Status**
 - RegistrationSummary
 - User Registrations
 - ▶ System Tools

- Shortcuts
- [Change Password](#)

Session Manager Downward Data Replication Status

This page allows you to view Session Manager downward data replication statistics and run tests.

Master Database and Session Manager Replica Database Statistics

Stat Name	Master	ASM1-DR (replica)	ASM2-DR (replica)
Records Currently in Database	1077	1077	1077
Records Pending Update	0	0	0
Modifications	1303	11783	27701
Modifications Resulting from Audits	1941	0	0
Failed Modifications (replica only)	N/A	0	0
Failed Modifications Resulting from Audit (replica only)	N/A	0	0
Elapsed Time Since Last Update/Audit (Days H:M:S)	00:00:04	00:12:49	00:15:42
Elapsed Time Since Last Update/Audit Requiring Modifications (Days H:M:S)	00:04:14	20 01:43:06	46 23:36:00
Last JMS Message Sent (master) / Received (replica)	Jan 4, 2010 2:33:56 PM MST	Jan 4, 2010 2:33:56 PM MST	Jan 4, 2010 2:33:56 PM MST
Last JMS Message Received (master) / Sent (replica)	Jan 4, 2010 2:25:21 PM MST	Jan 4, 2010 2:25:21 PM MST	Jan 4, 2010 2:22:28 PM MST
JMS Connection Status	OK	OK	OK
Test String Value	1111	1111	1111
Test String Last Update Time	Dec 22, 2009 2:51:26 PM MST	Dec 22, 2009 2:51:26 PM MST	Dec 22, 2009 2:51:26 PM MST

5.1.2. Verify SIP Link Status

Expand the Session Manager menu on the left and click SIP Entity Monitoring. Verify all SIP Entity Links are operational as shown below:



- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ **Session Manager**
 - Session Manager Administration
 - ▶ Network Configuration
 - ▶ Device and Location Configuration
 - ▶ Application Configuration
 - ▼ **System Status**
 - System State Administration
 - System State Monitoring
 - SIP Entity Monitoring**
 - Managed Bandwidth Usage
 - Security Module Status
 - Data Replication Status
 - RegistrationSummary
 - User Registrations
 - ▶ System Tools

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
ASM1-DR	0/8	0	0	0
ASM2-DR	0/0	0	0	0

All Monitored SIP Entities

8 Items Filter: Enable

SIP Entity Name
IPQ 500
Nortel-Node_Server
S8300-G450-FS
S8730-1
S8730-2
SIL-DR-MAS1
SIP Trunk to CUCM 5.0
VPMS

Select the corresponding SIP Entity for the Communication Manager Feature Server and verify the link is up as shown below:



- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ Session Manager
 - Session Manager Administration
 - ▶ Network Configuration
 - ▶ Device and Location Configuration
 - ▶ Application Configuration
 - ▼ System Status
 - System State Administration
 - ▶ SIP Entity Monitoring
 - Managed Bandwidth Usage

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: S8300-G450-FS

1 Item Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Hide	ASM1-DR	10.80.100.51	5060	TCP	Up	200 OK	Up
Time Last Down	Time Last Up	Last Message Sent	Last Response Latency (ms)				
Never	Dec 14, 2009 11:06:56 AM MST	Jan 4, 2010 3:00:36 PM MST	16				

5.1.3. Verify Registrations of SIP Endpoints

Verify SIP users have been created in the Session Manager. In the sample configuration, two SIP users were created as shown in the highlighted area below:



- ▶ Asset Management
 - ▶ Communication System Management
 - ▼ User Management
 - Manage Roles
 - User Management**
 - ▶ Global User Settings
 - Group Management
 - ▶ Monitoring
 - ▶ Network Routing Policy
 - ▶ Security
 - ▶ Applications
 - ▶ Settings
 - ▶ Session Manager
- Shortcuts**
- [Change Password](#)
 - [Help for View Users](#)

User Management

Users

[Advanced Search](#)

5 Items Filter: Enable

<input type="checkbox"/>	Status	Name	User Name	Handle	Last Login
<input type="checkbox"/>		Administrator	administrator@avaya.com		December 7, 2009 7:19:23 PM +06:00
<input type="checkbox"/>		Default Administrator	admin		December 15, 2009 10:30:29 PM +06:00
<input type="checkbox"/>		John Smith	6663000@avaya.com	6663000	
<input type="checkbox"/>		Jonez, Paul	6663001@avaya.com	6663001	
<input type="checkbox"/>		System User	system		

Select : All, None (0 of 5 Selected)

Verify the SIP endpoints have successfully registered with the Session Manager as shown below:



Home / Session Manager / System Status / User Registrations

- ▶ Asset Management
- ▶ Communication System Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ Session Manager
 - Session Manager Administration
 - ▶ Network Configuration
 - ▶ Device and Location Configuration
 - ▶ Application Configuration
 - ▼ System Status
 - System State Administration
 - SIP Entity Monitoring
 - Managed Bandwidth Usage
 - Security Module Status
 - Data Replication Status
 - RegistrationSummary
 - **User Registrations**
 - ▶ System Tools

Shortcuts

- [Change Password](#)
- [Help for User Registrations](#)
- [Help for Page Fields](#)

User Registrations

Select to send notifications to AST devices. Click on row to display registration detail.

Refresh AST Device Notifications: Reboot Reload ▾

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Registered	Address	Login Name	First Name	Last Name	Session Manager	AST Device
<input checked="" type="checkbox"/>	true	6663000@avaya.com	6663000@avaya.com	John	Smith	ASM1-DR	true
<input type="checkbox"/>	true	6663001@avaya.com	6663001@avaya.com	Paul	Jones	ASM1-DR	true
<input type="checkbox"/>	false	Administrator@avaya.com	administrator@avaya.com	SIL	Administrator	ASM1-DR	false

Select : All, None (1 of 3 Selected)

Registration Detail

Login Name: 6663000@avaya.com

Registration Address: 6663000@avaya.com

Registration Time: Wed Dec 16 13:41:47 MST 2009

Event Subscriptions:

- avaya-cm-feature-status
- dialog
- avaya-ccs-profile
- message-summary
- reg

User Communication Profile Addresses: 6663000@avaya.com

5.2. Verify Avaya Aura™ Communication Manager Feature Server Configuration

Verify the status of the SIP trunk group by using the “**status trunk n**” command, where “**n**” is the trunk group number administered in **Section 2.5**. Verify that all trunks are in the “in-service/idle” state as shown below:

```
status trunk 10
                TRUNK GROUP STATUS
Member  Port    Service State      Mtce Connected Ports
                Busy
0010/001 T00006  in-service/idle    no
0010/002 T00007  in-service/idle    no
0010/003 T00008  in-service/idle    no
0010/004 T00009  in-service/idle    no
0010/005 T00014  in-service/idle    no
0010/006 T00015  in-service/idle    no
0010/007 T00043  in-service/idle    no
0010/008 T00044  in-service/idle    no
0010/009 T00045  in-service/idle    no
0010/010 T00046  in-service/idle    no
```

Verify the status of the SIP signaling groups by using the “**status signaling-group n**” command, where “**n**” is the signaling group number administered in **Section 2.4**. Verify the signaling group is “in-service” as indicated in the **Group State** field shown below:

```

status signaling-group 10
                                STATUS SIGNALING GROUP

    Group ID: 10                    Active NCA-TSC Count: 0
    Group Type: sip                 Active CA-TSC Count: 0
    Signaling Type: facility associated signaling
    Group State: in-service
  
```

Use the Communication Manager SAT command, ‘**list trace tac #**’, where **tac #** is the trunk access code defined in **Section 2.5** to trace trunk group activity for the SIP trunk between the Session Manager and the Communication Manager Feature Server as shown below:

```

list trace tac #10                                     Page 1
                                LIST TRACE
time          data
11:01:01      Calling party station    6663000 cid 0x9e
11:01:01      Calling Number & Name 6663000 John Smith
11:01:01      active station          6663000 cid 0x9e
11:01:07      dial 6664000 route:UDP|AAR
11:01:07      term trunk-group 10    cid 0x9e
11:01:07      dial 6664000 route:UDP|AAR
11:01:07      route-pattern 10 preference 1 cid 0x9e
11:01:07      seize trunk-group 10 member 7 cid 0x9e
11:01:07      Calling Number & Name NO-CPNumber NO-CPName
11:01:07      Setup digits 6664000
11:01:07      Calling Number & Name 6663000 John Smith
11:01:07      Proceed trunk-group 10 member 7 cid 0x9e
11:01:07      Alert trunk-group 10 member 7 cid 0x9e
11:01:07      G711MU ss:off ps:20
  
```

Use the Communication Manager SAT command, 'list trace station xxx', where xxx is the extension number of the 96XX SIP telephone as shown below:

```
list trace station 6663000                                     Page 1
                                                                LIST TRACE
time                data
11:03:30           active station      6663000 cid 0x9f
11:03:33           dial 6664000 route:UDP|AAR
11:03:33           term trunk-group 10      cid 0x9f
11:03:33           dial 6664000 route:UDP|AAR
11:03:33           route-pattern 10 preference 1 cid 0x9f
11:03:33           seize trunk-group 10 member 8 cid 0x9f
11:03:33           Calling Number & Name NO-CPNumber NO-CPName
11:03:33           Setup digits 6664000
11:03:33           Calling Number & Name 6663000 John Smith
11:03:33           Proceed trunk-group 10 member 8 cid 0x9f
11:03:33           Alert trunk-group 10 member 8 cid 0x9f
11:03:33           G711MU ss:off ps:20
                    rgn:1 [10.80.111.13]:9808
                    rgn:1 [10.80.100.53]:2052
11:03:33           xoip options: fax:Relay modem:off tty:US uid:0x5002c
```

5.3. Call Scenarios Verified

Verification scenarios for the configuration described in these Application Notes included the following call scenarios:

- Place a call from a SIP phone registered to Session Manager to an extension on Communication Manger Access Element. Answer the call and verify talkpath.
- Place a call from an extension on the Communication Manger Access Element to a SIP phone registered to Session Manager. Answer the call and verify talkpath.
- Verify that calls can be transferred from a SIP phone registered to Session Manager to an extension on Communication Manager.
- Verify that calls can be transferred from an extension on Communication Manager Access Element to a SIP phone registered to Session Manager.
- Verify that a SIP phone registered to Session Manager can conference in extensions on Communication Manager Access Element.
- Verify extensions on Communication Manager Access Element can conference in SIP phones registered to Session Manager.

6. Acronyms

AAR	Automatic Alternative Routing (Routing on Communication Manager)
ARS	Alternative Routing Service (Routing on Communication Manager)
CLAN	Control LAN (Control Card in Communication Manager)
DCP	Digital Communications Protocol
DNIS	Dialed Number identification Service
DTMF	Dual Tone Multi Frequency
FQDN	Fully Qualified Domain Name (hostname for Domain Naming Resolution)
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSI	IP-services interface (Control Card in Communication Manager)
LAN	Local Area Network
MRCP	Media Resource Control Protocol
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SAT	System Access Terminal (Communication Administration Interface)
SIL	Solution Interoperability Lab
SIP	Session Initiation Protocol
SM	Avaya Aura™ Session Manager
SMGR	System Manager (used to configure Session Manager)
SNMP	Simple Network Management Protocol
SRE	SIP Routing Element
SSH	Secure Shell
SSL	Secure Socket Layer
TAC	Trunk Access Code (Communication Manager Trunk Access)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
URE	User Relation Element
URL	Uniform Resource Locator
WAN	Wide Area Network
XML	eXtensible Markup Language

7. Conclusion

These Application Notes describe how to configure the Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager Access Element and Avaya Aura™ Communication Manager operating as a Feature Server to support 9600-Series SIP Telephones. Interoperability testing included successfully making bi-directional calls between several different types of endpoints and use of various features including transfer and conference.

8. Additional References

This section references the product documentation relevant to these Application Notes.

Session Manager

- 1) Avaya Aura™ Session Manager Overview, Doc ID 03-603323, available at <http://support.avaya.com>.
- 2) Installing and Administering Avaya Aura™ Session Manager, Doc ID 03-603324, available at <http://support.avaya.com>.
- 3) Avaya Aura™ Session Manager Case Studies, dated January 2, 2010, available at <http://support.avaya.com>
- 4) Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.

Communication Manager

- 5) Hardware Description and Reference for Avaya Aura™ Communication Manager (COMCODE 555-245-207) http://support.avaya.com/elmodocs2/comm_mgr/r4_0/avayadoc/03_300151_6/245207_6/245207_6.pdf
- 6) SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206, May 2009, available at <http://support.avaya.com>.
- 7) Administering Avaya Aura™ Communication Manager, Doc ID 03-300509, May 2009, available at <http://support.avaya.com>.
- 8) Administering Avaya Aura™ Communication Manager as a Feature Server, Doc ID 03-603479, November 2009, available at <http://support.avaya.com>

©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabinotes@list.avaya.com